Applicants : Sydir et al.
Serial No. : 10/749,913
Filed : December 29, 2003
Page : 14 of 18

Attorney's Docket No.: INTEL-013PUS
Intel Docket No. P17940

REMARKS

Claims 42 to 50 and 52 to 78 are pending in this application of which claims 42, 52, 58, 63, 68 and 72 are the independent claims. Claim 51 is cancelled without prejudice. Favorable consideration and further examination are respectfully requested.

Claims 42, 44, 45, 48 to 53, 55, 56, 58, 60, 62, 63, 65 to 70 and 72 to 77 are rejected under 35 U.S.C. § 103(a) as being obvious over Ohta et al. (U.S. Patent Application Publication Number 2002/0083317 hereinafter "Ohta") in view of Tardo et al. (U.S. Patent Number 7,082,534). Claims 46, 47 and 54 and 61 are rejected under 35 U.S.C. § 103(a) as being obvious over Ohta in view of Tardo and in further view of Corder et al. (U.S. Patent Number 7,069,447). Claims 43, 57, 59, 64 and 71 are rejected under 35 U.S.C. § 103(a) as being obvious over Ohta in view of Tardo and in further view of Yoaz et al. ("Speculation Techniques for Improving Load related Instruction Scheduling" hereinafter "Yoaz")

The applied art is not understood to disclose or to suggest the foregoing features of claim 1. In particular, the cited references do not disclose or suggest that each buffer element has a size that is at least as large as a largest authentication algorithm block size implemented by the authentication cores (emphasis added).

The Examiner has indicated that Ohta teaches the limitation at paragraph [0011] citing "a data block accumulation unit that outputs the accumulated amount to the authentication processing unit when it reaches the smallest data block size for the authenticating processing" (emphasis added, see page 6 of the Office Action). The Examiner also points to FIGS. 1 and 2 of Ohta and their associated text as further support and stating that "(i)t would be only logical to

Applicants : Sydir et al.
Serial No. : 10/749,913
Filed : December 29, 2003
Page : 15 of 18

Attorney's Docket No.: INTEL-013PUS
Intel Docket No. P17940

have a buffer size that is large enough to accommodate the largest block size" (see page 6 of the Office Action). However, Ohta only describes <u>a single authentication core</u> in FIGS. 1 and 2 and therefore Ohta does not teach more than one authentication core much less authentication cores <u>requiring a different authentication algorithm block size</u>. Therefore, Ohta does not teach that each buffer element has a size that is at least as large as a <u>largest</u> authentication algorithm block size implemented by the authentication cores.

Tardo merely mentions different authentication algorithms. Tardo does not teach buffer elements much less a buffer element having a size that is at least as large as a largest authentication algorithm block size implemented by the authentication cores.

Accordingly, for at least the reasons indicated above, even if Tardo were combined with Ohta, the resulting hypothetical combination would not disclose or suggest that each buffer element has a size that is at least as large as a <u>largest</u> authentication algorithm block size implemented by the authentication cores. For example, even using Tardo's authentication cores and assuming more than one authentication core have different block sizes, Ohta clearly says that when the <u>smallest</u> data block size is achieved the data block it is outputted and not the <u>largest</u> authentication algorithm block size implemented by the authentication cores (see paragraph [0011] of Ohta).

Claims 52, 58, 63, 68 and 72 include the feature that each buffer element has a size that is at least as large as a largest authentication algorithm block size implemented by the authentication cores as in claim 42. Applicants submit that the Tardo and the Ohta references should also be withdrawn with respect to claims 52, 58, 63, 68 and 72 for at least the same reasons as claim 42.

Applicants : Sydir et al.   Attorney's Docket No.: INTEL-013PUS
Serial No. : 10/749,913   Intel Docket No. P17940
Filed   : December 29, 2003
Page   : 16 of 18

Furthermore, independent claims 58 and 68 along with dependent claims 44, 53, 65 and

77 include the limitation that one of the authentication cores processes data in 16-byte blocks and

another one of the authentication cores processes data in 64-byte blocks. The Examiner has

indicated that Ohta teaches this limitation at paragraph [0016] (see pages 6, 7 and 9 of the Office

Action), which states

> Here, in the above-mentioned security communication packet
> processing apparatus, the data block for the encryption processing can be
> 64 bits, and the data block for the authentication processing can be 512
> bits. In this case, the data block accumulation unit may output the data
> blocks when it accumulates eight encrypted data blocks.

However, Ohta mentions nothing about <u>two</u> authentication cores because Ohta only teaches a

single authentication core. Furthermore, the Examiner's statement that "outputting blocks of

data to the encryption and authentication processors in multiples of 8 bits, which include all

processing block in claims 8 and 9" (see pages 6 and 7 of the Office Action) is confusing since 8

bits is not even mention in the cited passage and should be explained further for the record since

even if it was in the cited passage the Examiner has not logically associated that statement with

the recited claims. As in the previous Office Action, Applicants respectfully request that the

Examiner once again explain this statement. Furthermore, Applicants respectfully submit that

the cited passage clearly only states 512 bits for authentication processing which, assuming 8 bits

per byte, is 64-bytes. Thus, there is not even a teaching that suggests encryption of 16-bytes in

the cited passage. Thus, Applicants respectfully submit that claims 44, 53, 58, 65, 68 and 77

should be allowed.

Moreover, independent claims 52 and 68 along with dependent claims 48, 60, 66 and 78

include the limitation that one of the cipher cores processes data in 8-byte blocks and another one

Applicants : Sydir et al.
Serial No. : 10/749,913
Filed : December 29, 2003
Page : 17 of 18

Attorney's Docket No.: INTEL-013PUS
Intel Docket No. P17940

of the cipher cores processes data in 16-byte blocks. The Examiner has indicated that Ohta teaches this limitation at paragraph [0016] (see pages 7 and 9 of the Office Action)). However, Ohta mentions nothing about two cipher cores because Ohta only teaches a single cipher core. Furthermore, the Examiner's statement that "outputting blocks of data to the encryption and authentication processors in multiples of 8 bits, which include all processing block in claims 44 and 45" (see page 7 of the Office Action) is, as mentioned previously confusing, and should be explained further for the record since the cited passage mentions nothing about 8 bits nor is the Examiner's statement rationally related to the recited claims. Furthermore, Applicants respectfully submit that the cited passage clearly only states 64 bits for encryption processing which, assuming 8 bits per byte, is 8-bytes. Thus, there is not a teaching that suggests encryption of 16-bytes in the cited passage. Thus, Applicants respectfully submit that claims 48, 52, 60, 66, 68 and 78 should be allowed.

For at least the foregoing reasons, Applicants request withdrawal of the art rejections.

Applicants submit that all dependent claims now depend on allowable independent claims.

It is believed that all of the pending claims have been addressed. However, the absence of a reply to a specific rejection, issue or comment does not signify agreement with or concession of that rejection, issue or comment. In addition, because the arguments made above may not be exhaustive, there may be reasons for withdrawing the prior art cited with regards to any or all pending claims (or other claims) that have not been expressed. Finally, nothing in this paper should be construed as intent to concede any issue with regard to any claim, except as

specifically stated in this paper, and the amendment of any claim does not necessarily signify

concession of unpatentability of the claim prior to its amendment.

Applicants submit that the entire application is now in condition for allowance. Such

action is respectfully requested at the Examiner's earliest convenience.

Applicants' attorney can be reached by telephone at (781) 401-9988 ext. 123.

No fee is believed to be due for this Response; however, if any fees are due, please apply

such fees to Deposit Account No. 50-0845 referencing Attorney Docket: INTEL-013PUS.

Respectfully submitted,

Date: 22 December 2007

Anthony T. Moosey
Reg. No. 55,773

Attorneys for Intel Corporation
Daly, Crowley, Mofford & Durkee, LLP
354A Turnpike Street - Suite 301A
Canton, MA 02021-2714
Telephone: (781) 401-9988 ext. 123
Facsimile: (781) 401-9966